media replacement, etc.). The information recorded must be used when reviewing performance reports to ensure that the maintenance or modifications did not improperly affect the data in the reports.

(6) *Statistical reporting.* (i) The bingo sales, prize payouts, bingo win, and actual bingo win percentages must be recorded for:

(A) Each shift or session;

(B) Each day;

(C) Month-to-date; and

(D) Year-to-date or fiscal year-to-date.

(ii) A monthly comparison for reasonableness must be made of the amount of bingo paper sold from the bingo paper control log to the amount of bingo paper sales revenue recognized.

(iii) Management employees independent of the bingo department must review bingo statistical information on at least a monthly basis.

(iv) Agents independent of the bingo department must investigate any large or unusual statistical fluctuations, as defined by the gaming operation.

(v) Such investigations must be documented, maintained for inspection, and provided to the tribal gaming regulatory authority upon request.

(vi) The actual bingo win percentages used in the statistical reports should not include operating expenses (*e.g.*, a percentage payment to administrators of inter-tribal prize pools), promotional prize payouts or bonus payouts not included in the prize schedule.

(7) *Progressive prize pools.* (i) A display that shows the amount of the progressive prize must be conspicuously displayed at or near the player interface(s) to which the prize applies.

(ii) At least once each day, each gaming operation must record the total amount of each progressive prize pool offered at the gaming operation on the progressive log.

(iii) When a manual payment for a progressive prize is made from a progressive prize pool, the amount must be recorded on the progressive log.

(iv) Each gaming operation must record, on the progressive log, the base reset amount of each progressive prize the gaming operation offers.

(v) Procedures must be established and implemented specific to the transfer of progressive amounts in excess of the base reset amount to other awards or prizes. Such procedures may also include other methods of distribution that accrue to the benefit of the gaming public.

§§ 543.8–543.15 [Reserved]

§ 543.16 What are the minimum internal controls for information technology?

(a) Physical security measures restricting access to agents, including vendors, must exist over the servers, including computer terminals, storage media, software and data files to prevent unauthorized access and loss of integrity of data and processing.

(b) Unauthorized individuals must be precluded from having access to the secured computer area(s).

(c) *User controls.* (1) Computer systems, including application software, must be secured through the use of passwords or other approved means.

(2) Procedures must be established and implemented to ensure that management or independent agents assign and control access to computer system functions.

(3) Passwords must be controlled as follows unless otherwise addressed in the standards in this section.

(i) Each user must have his or her own individual user identification and password.

(ii) When an individual has multiple user profiles, only one user profile per application may be used at a time.

(iii) Passwords must be changed at least quarterly with changes documented. Documentation is not required if the system prompts users to change passwords and then denies access if the change is not completed.

(iv) The system must be updated to change the status of terminated users from active to inactive status within 72 hours of termination.

(v) At least quarterly, independent agents must review user access records for appropriate assignment of access and to ensure that terminated users do not have access to system functions.

(vi) Documentation of the quarterly user access review must be maintained.

(vii) System exception information (*e.g.*, changes to system parameters, corrections, overrides, voids, etc.) must be maintained.

(4) Procedures must be established and implemented to ensure access listings are maintained which include at a minimum:

(i) User name or identification number (or equivalent); and

(ii) Listing of functions the user can perform or equivalent means of identifying same.

(d) Adequate backup and recovery procedures must be in place that include:

(1) *Daily backup of data files*—(i) *Backup of all programs.* Backup of programs is not required if the program can be reinstalled.

(ii) Secured storage of all backup data files and programs, or other adequate protection to prevent the permanent loss of any data.

(iii) Backup data files and programs may be stored in a secured manner in another building that is physically separated from the building where the system's hardware and software are located. They may also be stored in the same building as the hardware/software as long as they are secured in a fireproof safe or some other manner that will ensure the safety of the files and programs in the event of a fire or other disaster.

(2) Recovery procedures must be tested on a sample basis at least annually with documentation of results.

(e) *Access records.* (1) Procedures must be established to ensure computer access records, if capable of being generated by the computer system, are reviewed for propriety for the following at a minimum:

(i) Class II gaming systems;

(ii) Accounting/auditing systems;

(iii) Cashless systems;

(iv) Voucher systems;

(v) Player tracking systems; and

(vi) External bonusing systems.

(2) If the computer system cannot deny access after a predetermined number of consecutive unsuccessful attempts to log on, the system must record unsuccessful log on attempts.

(f) *Remote access controls.* (1) For computer systems that can be accessed remotely, the written system of internal controls must specifically address remote access procedures including, at a minimum:

(i) Record the application remotely accessed, authorized user's name and business address and version number, if applicable;

(ii) Require approved secured connection;

(iii) The procedures used in establishing and using passwords to allow authorized users to access the computer system through remote access;

(iv) The agents involved and procedures performed to enable the physical connection to the computer system when the authorized user requires access to the system through remote access; and

(v) The agents involved and procedures performed to ensure the remote access connection is disconnected when the remote access is no longer required.

(2) In the event of remote access, the information technology employees must prepare a complete record of the access to include:

(i) Name or identifier of the employee authorizing access;

(ii) Name or identifier of the authorized user accessing system;

(iii) Date, time, and duration of access; and

(iv) Description of work performed in adequate detail to include the old and new version numbers, if applicable of any software that was modified, and details regarding any other changes made to the system.

PARTS 544–546 [RESERVED]

PART 547—MINIMUM TECHNICAL STANDARDS FOR GAMING EQUIPMENT USED WITH THE PLAY OF CLASS II GAMES

Sec.